access to.

U.S. patent 6098056 shows a method for controlling access to data through the Internet. A server is coupled to a storage device for storing the data which is encrypted using a random generated key. This is further encrypted with the server's public key. A trusted information handler is validated by the server. After the handler has been authenticated, the server key decrypts the data with its private key and re-encrypts the data with the handler's public key.

U.S. patent 6289455 shows a cryptographic method to regulate access to data. Rights keys which allow access to the data are added to a cryptographic unit by transforming data received from a control processor and storing the result. The unit then produces content decrypting keys by storing rights keys to transform other data received from a processor. Because the processor design has the ability to directly access the protected memory, security can remain effective even if the processor is compromised.

U.S. patent 5673316 shows a method to control access to data using cryptographic envelopes. An envelope is an aggregation of information parts, where each of the parts to be protected are encrypted with a corresponding part encryption key. Each part encryption key is also encrypted with a public key.

U.S. patent 4914698 shows method for issuing blind digital signatures which are untraceable.

International PCT published application 01/22760 shows a system for setting up a wireless transmission connection transmit identification messages.

While the prior art shows a number of different types of key and lock arrangements, they are all subject to a number of shortcomings by requiring the carrying of a number of keys or knowing various codes.

Summary of the Invention

One aspect of the present invention is to provide a wireless lock and key system.

Another aspect of the present invention is to provide a wireless lock and key system which utilizes an encryption key pair.

A further aspect of the present invention is to provide a wireless lock and key system having the ability to generate tickets to be used by other authorized persons.

A still further aspect of the present invention is to provide a wireless lock and key system where a single key may be used with a plurality of locks.

Another aspect of the present invention is to provide a wireless lock and key system which further includes a control device for loading data into the key.

Another aspect of the invention is to provide a method for managing and controlling locks, which increases security and enables creation of temporary or otherwise limited, easily distributable keys (also referred to as "tickets"). .

In accordance with the embodiment of the invention, digital signatures and public key cryptography are used to solve the problems mentioned in the previous sections. Each user has a key device. Preferably a user has only one key device in use at a time. Key devices contain both a public and a secret key (hereafter a public key - secret key combination is referred to as an RSA key pair. However, some other public key cryptosystem could also be used. Lock devices contain the public keys of all the users that have permission to open the lock. Additionally, separate control devices may be used for

controlling lock and key devices to minimize the need for control panels, allowing key and lock devices to be small.

In the preferred embodiment of the invention, wireless communication is used between lock devices, key devices and control devices. The wireless communication devices are preferably short range communication like Bluetooth devices, for reasons of price, power consumption, compatibility and size. In the following, it is assumed that Bluetooth devices are used, as the described methods utilize Bluetooth security features. However, other systems that offer basic authentication and encryption support could also be used.

A user is given the right to open a lock ("given a key") by storing the public key of the user's key device on the lock. Note that in this way a key device can open an infinite amount of locks, but only needs to store one RSA key pair. Also, the owner of a lock is unable to open any other locks the key device can open, since he only knows the public key of the key device.

When a key device detects a nearby lock device, it requests access. The lock device issues a challenge in the form of a random code. The key device encrypts the code with its secret key, and sends the result to the lock, who decrypts it with the public key of the key device that was stored in the lock earlier. If the decrypted code is the same that the lock device originally sent, the lock opens.

Access permissions, or "tickets" can be created by specifying a list of limitations (such as who is able to use the permission and when), and digitally signing the permission with the secret key of a user that has access to the lock in question (meaning, his public key is stored in the lock). The lock is then able to verify that the permission was created by a user authorized to do so. Since the ticket can be limited to